Listing of Claims:

1. (Currently Amended) A database system regulating access to one or more data records according to authorized access rights, the database system comprising:

one or more data crystals storing one or more data records in an obfuscated format;

one or more iterators, each iterator programmed to access, deobfuscate, and return at least one of the one or more data records in response to a data request;

one or more queries, each query predefined to receive an indication of an authorized type of data requirement, to request at least one data record from the iterator, and to select from among the returned at least one data record a requested data record satisfying the data requirement; and

a key crystal granting access rights for the database system

whereby the one or more data crystals, one or more iterators, one or more queries, and key crystal regulate access to the one or more data records.

2. (Original) The database system of claim 1 further comprising an application to provide the indication of the data requirement to the one or more queries, wherein the application has direct access to the one or more queries but not the one or more iterators, the one or more data crystals, or the one or more data records.

3. (Original) The database system of claim 2 wherein the application selects among the one or more queries based on the type of data requirement.

4. (Original) The database system of claim 1 wherein the obfuscated format is chosen from the group consisting of: compression, encryption, XOR operations, and general bit order or bit logical manipulation.

5. (Original) The database system of claim 4 wherein the obfuscated format is compression so as to reduce memory requirements for the storing of the one or more data records.

6. (Original) The database system of claim 1, further comprising an iterator interface corresponding to a specific iterator and a corresponding data crystal; and

wherein:

the iterator interface acts as a buffer between the one or more queries and the corresponding iterator; and

the iterator interface allows the queries to work with a different version of the specific iterator and corresponding data crystal.

7. (Original) The database system of claim 1, further comprising an access key for interchangeably enabling or disabling the system.

8. (Original) The database system of claim 7 wherein the access key is a hardware dongle.

9. (Original) The database system of claim 7 wherein the access key is a software component.

10. (Original) The database system of claim 1 wherein at least one data record includes a link to an external storage location.

11. (Original) The database system of claim 1 wherein at least one of the one or more data records includes unobfuscated clear text.

12. (Original) The database system of claim 1 wherein:

the one or more data records include a first data record and a second data record;

the first data record employs a first obfuscated format and the second data record employs a second obfuscated format; and

the second obfuscated format is different than the first obfuscated format.

13. (Original) The database system of claim 1 further comprising a viewer to view a select data record without enabling full access to all of the one or more data records.

14. (Original) The database system of claim 1 wherein the one or more data crystals, the one or more iterators, and the one or more queries are deployed at an unsecured customer location.

15. (Original) The database system of claim 1 wherein each iterator corresponds to only one of the one or more data crystals.

16. (Original) The database system of claim 1 wherein a first query can call a second query to employ at least one of the one or more iterators.

17. (Currently Amended) A controlled access database system comprising:

a plurality of data crystals, each data crystal containing at least one data record employing an obfuscation technique;

an iterator programmed to access the at least one data record according to the obfuscation technique;

at least one query of a predefined type:

wherein one or more of the at least one query is called by an application with a data requirement;

wherein the data requirement of the application determines the one or more called query; and

wherein the one or more called query employs the iterator to access the at least one data record; and

a key crystal granting access rights to the database system

whereby the plurality of data crystals, iterator, at least one query, and key crystal control access to the at least one data record.

18. (Currently Amended) The database system of claim 17 wherein the key crystal authorizes access to a specific data crystal~~specific data crystals~~ out of the plurality of data crystals, wherein the specific data crystal is authorized for the application.

19. (Original) The database system of claim 17 wherein the key crystal authorizes access to a specific query out of the at least one query, wherein the specific query is authorized for the application.

20. (Original) The database system of claim 17 wherein a first query can call a second query to employ the iterator.

21. (Original) A method for building a controlled-access database for preventing unauthorized access to data records, the method comprising the steps of:

obtaining a data record;

storing the data record in a data crystal in an obfuscated format;

providing an iterator to access and deobfuscate the obfuscated data record;

providing a query to request the iterator to locate and access the data record only in accordance with a preauthorized type of data requirement; and

providing a key crystal authorizing use of the data crystal and the query according to the preauthorized type of data requirement

whereby the data crystal, iterator, query, and key crystal prevent unauthorized access to the data record.

22. (New) A method for accessing data stored in a secure database comprising:

receiving a request for data, the data stored in an obfuscated format within a data crystal;

determining an accessible predefined query based upon query permissions stored within a key crystal; and

calling the accessible predefined query to direct an iterator to access, deobfuscate, and return data satisfying the request so that the data stored within the data crystal remains secure.

23. (New) The method of claim 22 further comprising determining an accessible data crystal based upon crystal permissions stored within the key crystal and wherein the iterator accesses, deobfuscates, and returns the data from the accessible data crystals.

24. (New) The method of claim 22 wherein the request is received from a parser application of an automated data capture and perfection system.

25. (New) The method of claim 22 wherein the data corresponds to data fields of an address.

26. (New) The method of claim 22 further comprising:

receiving a second request for data;

calling the accessible predefined query to direct an iterator to access, deobfuscate, and return the data satisfying the second request; and

selecting a result based upon a correlation between the data satisfying the request and the data satisfying the second request.

27. (New) The database system of claim 1 wherein the data requirement corresponds to a data field of an address.

28. (New) The database system of claim 1 wherein the access rights include query permissions to determine which of the one or more queries are accessible.

29. (New) The database system of claim 1 wherein the access rights include crystal permissions to determine which of the one or more data crystals are accessible.

30. (New) The method of claim 21 wherein the data requirement corresponds to a data field of an address.